Strategies for Firmware Support of Self-Encrypting Drives

UEFI Winter Plugfest – February 21-23, 2011
Presented by Jeff Bobzin
(Insyde Software, Inc.)
Agenda

- Background
- System Firmware Flows
- UEFI Storage Security Command
- Plan for Older OS
- Partner Coordination
- Questions
Background:
TCG OPAL Self-Encrypting Drives
Terms and Definitions

• TCG = Trusted Computing Group
• OPAL = Specification Of Security Storage Class published by TCG
• eDrive = Feature name coined by MS
• IEEE1667 = Related spec for Removables
• Banding = Encrypted Range on Drive
Typical Banding

UEFI System Partition
Not Encrypted

OS Recovery
Not Encrypted

UEFI OS Partition
Encrypted Band

OEM Tools Partition
Not Encrypted
New System Firmware Flows
POST Flow Chart

See if the ATA device support trust computing feature or not. If yes, then install Storage Security Protocol at the ATA device handle.

Install Protocol

Storage Security Command Protocol

Storage Security Command Driver

Verify eDrive

bit 0 of word 48 in IDENTIFY DEVICE data
Initial Drive Encryption

Encryption with OPAL disk h/w encryption only needs several seconds. This step performed in OS.

- AES-256
- Several seconds
- USB Key
- TPM Chip

UEFI OS
The UEFI Operating System Bootloader is responsible for unlocking the protected bands via the *Storage Security Command Protocol*. Unlock data is based on User Password or TPM measurements or both.
TPer Reset Flow

This is to prevent the scenario where the system is accidentally rebooting into a malicious environment that gains access to the unlocked protected bands. TCG Working Group defines two simple mechanisms allowing the BIOS to “reset” eDrives during restart.

• TPer Reset through IEEE 1667 protocol.
• TPer Reset through native TCG protocol.

TPer = Trusted Peripheral

After Reset, F/w locks all protected bands

TPer Reset through native TCG Protocol

POST(UEFI BIOS)

UEFI OS

UEFI Boot Loader

UEFI OS

NEW!
Typical Recovery Flow

UEFI OS Boot Loader

Locked Band with Problem

Unlocked UEFI Sys Part

Unlocked Recovery Tools

Drive Bands

UEFI Recovery
UEFI Storage Security Command Protocol
Storage Security Command Protocol

This protocol is used to abstract mass storage devices to allow code running in the EFI boot services environment to send security protocol commands to mass storage devices without specific knowledge of the type of device or controller that manages the device. Functions are defined to send or retrieve security protocol defined data to and from mass storage devices. This protocol shall be supported on all physical and logical storage devices supporting the EFI_BLOCK_IO_PROTOCOL in the EFI boot services environment and one of the following command sets (or their alternative) at the bus level.

- TRUSTED SEND/RECEIVE commands of the ATA8-ACS command set or its successor
- SECURITY PROTOCOL IN/OUT commands of the SPC-4 command set or its successor. (SPC-4 : SCSI Primary Commands - 4)

UEFI Plugfest – February 2012
www.uefi.org
Protocol Interface Structure

- Protocol Interface Structure
  
  ```c
  typedef struct _EFI_STORAGE_SECURITY_COMMAND_PROTOCOL {
    EFI_STORAGE_SECURITY_RECEIVE_DATA ReceiveData;
    EFI_STORAGE_SECURITY_SEND_DATA SendData;
  } EFI_STORAGE_SECURITY_COMMAND_PROTOCOL;
  ```

- **ReceiveData()**
  Send a security protocol command to a device that receives data and/or the result of one or more commands sent by `SendData`.

- **SendData()**
  Send a security protocol command to a device.
Planning for users with Older OS Requirement
Older OS Validation

• Possible to use old-style BIOS whole-drive lock
  – Most Drive Manufacturers will still support the older Whole-Drive Password Feature on OPAL drives
  – No Expense to user but no recovery for lost password
Adding OPAL Support to Older OS

• Several ISV Packages available...
  A few examples:

1. Embassy ® Trusted Drive Manager from Wave Systems (www.wave.com)
   (For Windows XP, Vista, 7)

2. SecureDoc Full Disk Encryption from Winmagic (www.winmagic.com)
   (For Windows, Mac and Linux)
Partner Coordination
Bare-metal Restore Software

• The boot disk of any supported Restore Software will need tools to unlock the band to be restored!
  – Big changes for Tool – UEFI booting and OPAL unlock
  – OEM needs to confirm coordination between favorite OS and B/R vendors
Repair and Return

• Need to make sure training and procedures are in place for repair contractor handling of drives locked by consumer

• Need Field Service Tool to return drive to blank (all data lost)
SUMMARY

• TCG OPAL Drives provide High Security with great convenience
• UEFI 2.3.1 provides smooth boot path for UEFI OS
• OEMs need to consider Ecosystem Partners in OPAL Deployments
Thanks for attending the UEFI Winter Plugfest 2012

For more information on the Unified EFI Forum and UEFI Specifications, visit http://www.uefi.org

presented by